

Article

Complex Wavelet-Based Image Watermarking with the Human Visual Saliency Model

Jinhua Liu ^{1,*} , Yunbo Rao ² and Yuanyuan Huang ³¹ School of Mathematics and Computer Science, Shangrao Normal University, Shangrao 334001, China² School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China; raoyb@uestc.edu.cn³ Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, China; hy@cuit.edu.cn

* Correspondence: liujinhua_uestc@126.com

Received: 28 October 2019; Accepted: 28 November 2019; Published: 2 December 2019



Abstract: Imperceptibility and robustness are the two complementary, but fundamental requirements of any digital image watermarking method. To improve the invisibility and robustness of multiplicative image watermarking, a complex wavelet based watermarking algorithm is proposed by using the human visual texture masking and visual saliency model. First, image blocks with high entropy are selected as the watermark embedding space to achieve imperceptibility. Then, an adaptive multiplicative watermark embedding strength factor is designed by utilizing texture masking and visual saliency to enhance robustness. Furthermore, the complex wavelet coefficients of the low frequency sub-band are modeled by a Gaussian distribution, and a watermark decoding method is proposed based on the maximum likelihood criterion. Finally, the effectiveness of the watermarking is validated by using the peak signal-to-noise ratio (PSNR) and the structural similarity index measure (SSIM) through experiments. Simulation results demonstrate the invisibility of the proposed method and its strong robustness against various attacks, including additive noise, image filtering, JPEG compression, amplitude scaling, rotation attack, and combinational attack.

Keywords: image watermarking; visual saliency; image entropy; dual tree complex wavelet transform; structural similarity

1. Introduction

With the growing popularity of big data and multimedia applications, a large number of digital multimedia data are generated, transmitted, and distributed over the Internet every day. The security of these digital data is a relevant problem. An efficient solution is watermarking technology, which is mainly used for copyright protection, authentication, fingerprinting, etc. [1–3]. In general, the main idea of digital watermarking is to embed useful information in a host signal without affecting the perceptual quality of the host signal. For a watermarking method, the three indispensable, but conflicting requirements are robustness, invisibility, and capacity [1]. These requirements are mutually reinforcing and have to be solved together. For instance, when the imperceptibility of watermarking is improved, the robustness of watermarking will be reduced. Therefore, an ideal digital watermarking should achieve good balance among these three requirements.

To achieve the above goal, extensive watermarking methods have been proposed in recent years. These methods can be classified in different ways, e.g., spatial domain methods [4] and frequency domain methods [5–9], based on watermark embedding space. Depending on the manner of embedding, the method can be further categorized into additive [10], multiplicative [11,12],

and quantization based methods [13,14]. In addition, the watermarking methods can be categorized as blind [11] and non-blind [15] ones based on watermark decoding.

In terms of embedding region, most current watermarking methods focus on the frequency domain [6,7,16], because frequency domain watermarking algorithms are relatively more robust, invisible, and stable, especially the wavelet based watermarking [16]. The reason is that wavelet based watermarking has two obvious advantages. One of the advantages is that the wavelet transform fits well with the human visual system, which can be exploited in the design of an invisible watermarking [17–21]. The other advantage is that the wavelet transform has good multi-scale analytic characteristics, which can be used to develop a robust watermarking method [21–24]. Subsequently, many watermarking methods that use wavelets have been proposed in the past two decades. In terms of embedding method, the multiplicative watermarking methods are reportedly more robust, and they provide higher imperceptibility than the additive ones [25,26]. The multiplicative watermarking approaches are dependent on image content [25], and more importantly, they have strong robustness. Therefore, multiplicative watermarking methods are preferred for copyright protection [26]. For this reason, the multiplicative embedding approach is adopted in our study.

The wavelet transform has the advantages of the localization of the time frequency and multi-scale analysis, and it is suitable for describing the characteristics of 1D signals. However, when the signal dimension increases, the wavelet transform cannot sufficiently describe the singularity of the signal [27]. Therefore, to capture the direction information of 2D signals, multi-scale geometric analytic techniques for obtaining the intrinsic geometric structure information of images, such as contours and smooth curves, have emerged in recent years. These technologies include the ridgelets [15,28], wave atoms [29], contourlets [27,30], framelets [31], and dual tree-complex wavelet transform (DT-CWT) [32,33].

Current watermarking algorithms, such as the methods in [16,28,30], have achieved satisfying results; however, some problems need to be solved. Akhaee et al. [16] proposed a robust scaling based watermarking with the multi-objective optimization approach. Although the balance of invisibility and robustness of watermarking has been elaborately addressed by the method [16], the cost of multi-objective optimization is high, which hinders its extension to real applications. Despite the success of the multi-scale geometric analysis technology in various image watermarking-like methods [9,30], the time cost of these methods is also high. As a result, designing a simple and effective digital watermarking method to balance robustness and imperceptibility is necessary.

In addressing the above issues, the quantization watermarking approach with the L1 norm function was proposed in our previous work [33]. This work achieved good imperceptibility, but the robustness of the watermark against some attacks remains insufficient. In the present study, a watermarking that can be easily implemented is developed, and the robustness of watermarking is boosted based on the visual perception model. In this manner, the fidelity of the image can be improved. The developed method can achieve a good balance between invisibility and robustness of watermarking, which is beneficial to the practical use of watermarking technology.

DT-CWT is regarded as an overcomplete transform, which creates redundant complex wavelet coefficients that can be utilized to embed watermarks. In general, shift invariance is the main feature of DT-CWT. We can use this property to produce a watermark that can be decoded even after the host signal has undergone geometric attacks, such as amplitude scaling and rotation. DT-CWT also has good directional selectivity. Therefore, we propose an image watermarking by using DT-CWT in this paper. First, we segment the original image and choose the image blocks with high entropy in this study. Second, we embed watermark data into the low frequency of the complex wavelet coefficients by a visual perceptual model, and we extract the watermark data by using the maximum likelihood estimator (MLE). Finally, we validate the effectiveness of the watermarking algorithm through experimental simulation.

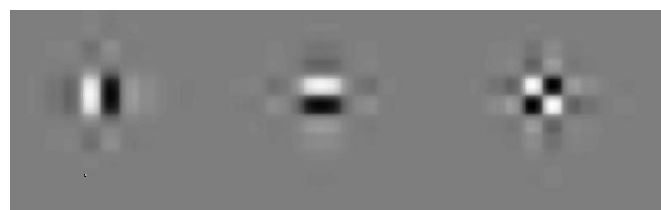
The contributions of the proposed method are twofold. On the one hand, an adaptive watermark embedding method in terms of texture masking and the visual saliency model is developed, which embeds each watermark bit into a set of dual tree complex wavelet coefficients. Using this

strategy, the robustness and imperceptibility of the watermark can be well balanced. On the other hand, the low frequency of complex coefficients with high entropy is selected as the watermark embedding space, which can improve the robustness of watermarking against some geometric attacks, such as rotation, scaling, and combinational attack.

The rest of the paper is structured as follows. Section 2 provides the basic concept of DT-CWT. Section 3 introduces the proposed watermarking method, including watermark embedding and watermark decoding. We test and discuss the performance of the proposed watermarking through experiments, and the corresponding findings are discussed in Section 4. The conclusion is presented in Section 5.

2. Dual Tree-Complex Wavelet Transform

DT-CWT, which was initially proposed by Selesnick, Baraniuk, and Kingsbury [32], inherits the characteristics of wavelets, and it can approximate shift invariances and has good directional selectivity [32]. A DT-CWT with a wavelet transform can produce six directional sub-bands oriented at 75° , 15° , -45° , -75° , -15° , and 45° on a decomposition scale. By contrast, a wavelet transform only has three directional sub-bands oriented at 90° , 0° , and 45° on a scale. A comparison of the impulse responses of these two wavelet transforms is shown in Figure 1. As mentioned above, DT-CWT can effectively approximate shift invariances. This invariance can be used to design watermarking, which then can be used to counter geometric attacks. For instance, if the image block is re-sampled after scaling, then DT-CWT can generate a set of coefficients that are roughly the same as the original patch. This scheme enables the watermarking to counter scaling attacks. Transformations, such as discrete wavelet transform (DWT), discrete cosine transform (DCT), and Fourier transform, do not have this property.



(a) DWT



(b) DT-CWT

Figure 1. Impulse responses of the reconstruction filters in two transforms. (a) DWT. (b) DT-complex wavelet transform (CWT).

For a 1D signal, the wavelet coefficients obtained by using two filter trees are twice those of the original wavelet transform. Furthermore, the 1D signal can be decomposed by the 1D DT-CWT with a shifted and dilated mother wavelet function and scaling function [34], i.e.,

$$f(x) = \sum_{l \in \mathbb{Z}} s_{j_0,l} \varphi_{j_0,l}(x) + \sum_{j \geq j_0} \sum_{l \in \mathbb{Z}} c_{j,l} \psi_{j,l}(x), \quad (1)$$

where \mathbb{Z} denotes the set of natural numbers; J and l refer to the indices of shifts and dilations, respectively; $s_{j_0,l}$ denotes the scaling coefficient; and $c_{j,l}$ is the complex wavelet transform coefficient with $\varphi_{j_0,l}(x) = \varphi_{j_0,l}^r(x) + \sqrt{-1}\varphi_{j_0,l}^i(x)$ and $\psi_{j,l}(x) = \psi_{j,l}^r(x) + \sqrt{-1}\psi_{j,l}^i(x)$, where r and i represent the real and imaginary parts, respectively.

Figure 2 shows the calculation process of the real part and the imaginary part of DT-CWT. For tree a, filters h_0 and h_1 are used to compute the real part. For tree b, filters g_0 and g_1 are utilized to calculate the imaginary part. As shown in Figure 2, the output of the two trees can be interpreted as the real part and the imaginary part of the complex wavelet coefficients. For a 2D signal, a 2D image $f(x, y)$ can be decomposed by 2D DT-CWT [34], i.e.,

$$f(x, y) = \sum_{l \in \mathbb{Z}^2} s_{j_0,l} \varphi_{j_0,l}(x, y) + \sum_{\theta \in \Theta} \sum_{j \geq j_0} \sum_{l \in \mathbb{Z}^2} c_{j,l}^{\theta} \psi_{j,l}^{\theta}(x, y), \quad (2)$$

where $\theta \in \Theta = \{\pm 15^\circ, \pm 45^\circ, \pm 75^\circ\}$ denotes the directionality of DT-CWT. At each scale of decomposition, the DT-CWT decomposition of $f(x, y)$ results in six complex valued high pass sub-bands in which each high pass sub-band corresponds to one unique direction θ .

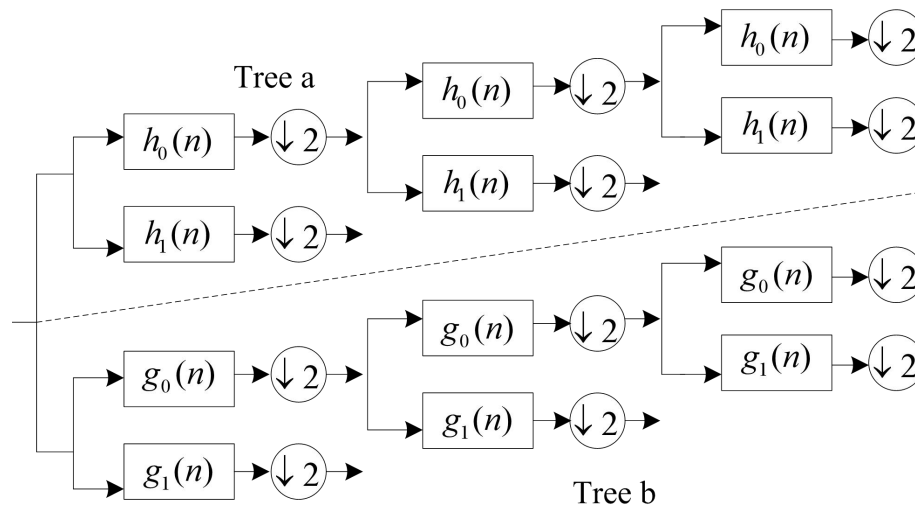


Figure 2. Two-level 1D dual tree complex wavelet transform.

3. Watermark Embedding and Detection

Human eyes are generally less sensitive to high entropy image blocks than smooth ones based on the human visual perception model. The reason is that relatively strong edges usually appear in high entropy image blocks [35]. Inspired by [35], we propose an image watermarking method by using high entropy blocks in this work. The block diagram of the proposed method is illustrated in Figure 3, which consists of watermark encoding and watermark decoding. The main advantage of this proposed method is its simple implementation; moreover, the tradeoff between invisibility and robustness can be resolved by a visual perceptual model. DT-CWT is also adopted in this work to embed watermark information, which can improve the robustness of the watermarking against geometric attacks.

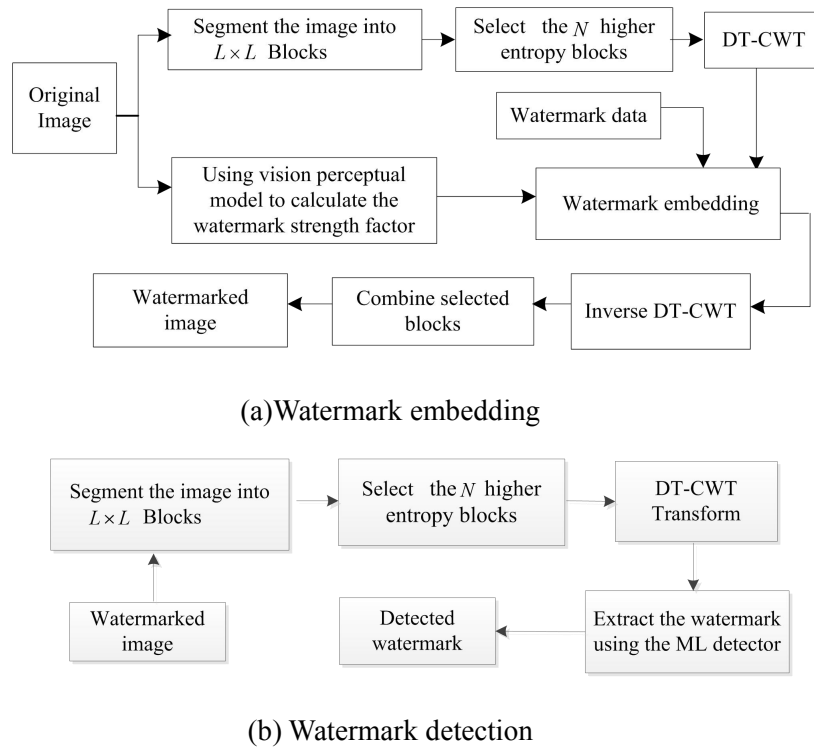


Figure 3. Block diagram of the proposed watermarking. (a) Embedding. (b) detection.

3.1. Watermark Embedding

As shown in Figure 3a. The procedure of the watermark embedding involves the following steps:

Step 1: The original image is segmented into blocks, and the first blocks in the ascending order of estimated entropy are selected for watermarking purposes.

Step 2: DT-CWT is applied to each selected image block, and a single bit of “0” or “1” is embedded in each block by manipulating the complex wavelet coefficients of the low frequency sub-band as follows:

$$\tilde{y} = x \times (1 + \alpha), \quad \text{for embedding 1,} \quad (3)$$

$$\tilde{y} = x \times (1 - \alpha), \quad \text{for embedding 0,} \quad (4)$$

where x denotes the host coefficients of the low frequency sub-band; \tilde{y} denotes the modified coefficients; and α is called the watermark strength factor, its value being determined by texture masking and visual saliency in Section 3.2.

Step 3: Repeat Step 2 for each image block.

Step 4: The inverse DT-CWT is applied to the watermarked blocks, and the watermarked blocks are combined with the non-watermarked blocks to obtain the whole watermarked image.

3.2. Visual Saliency Based Watermark Strength Factor

The watermark strength factor α can affect imperceptibility. To achieve the transparency of the watermark, two important concepts, texture masking and visual saliency, are used to design the watermark strength factor. The just noticeable difference (JND) threshold is often high in the texture region of an image [36]. Therefore, a high watermark strength factor can be selected to embed more information in the texture region. In addition. The work in [37] studied the spread transform dither modulation (STDMD) watermarking algorithm based on the visual saliency model and achieved good results. Furthermore, Wang et al. studied the JND estimation algorithm based on visual saliency in the wavelet domain [38]. The work in [39] utilized the JND scheme in designing a watermarking method. Besides this, in [40], an adaptive quantization watermarking algorithm was proposed. The term

“adaptive” in their work [40] was mainly used to describe a process, behavior, and/or a system that is able to interact with its environment. However, in our work, “adaptive” describes the embedding strength of watermark. As a result, the concept of visual saliency [38,41,42] is used to develop an adaptive watermark strength factor in this work. The human eye is inclined to focus on prominent areas, and distortions are more likely hidden in the area far from the image saliency part. However, watermark embedding strength can be enhanced accordingly. The watermark strength factor can be calculated as follows.

First, on the basis of the characteristic of the texture masking, the high frequency energy of the i^{th} image block is calculated by Equation (5), i.e., the value is the average of the sum of the energies of the six high frequency sub-bands.

$$E_{HF,i} = \frac{1}{6} (E_{H,1} + E_{H,2} + \dots + E_{H,6}), \quad (5)$$

where the six sub-bands of $E_{H,1}, E_{H,2}, \dots, E_{H,6}$ are produced, which correspond to the outputs of the six directional sub-bands oriented at $15^\circ, 45^\circ, 75^\circ, -15^\circ, -45^\circ$, and -75° . Subsequently, the high frequency sub-band image energy of the N image sub-block is computed as follows:

$$E_{HF} = \frac{1}{N} \sum_{i=1}^N E_{HF,i}, \quad (6)$$

where E_{HF} is the average energy of all image blocks. The watermark strength factor can increase with increasing E_{HF} . Hence, the high frequency portion of the watermark strength factor α_1 can be computed by employing the relationship proposed in [36] as follows:

$$\alpha_1 = a - c \times \exp(-\xi \cdot E_{HF}), \quad (7)$$

where the values of a , c , and ξ are set to 1.023, 0.02, and 3.5×10^{-5} , respectively.

According to [42], the final strength factor α can be computed by exploiting visual saliency. First, saliency distance is calculated for each image block, as denoted by D , and the maximum saliency distance is determined from the image blocks, as denoted by D_{\max} . In this manner, the visual saliency based strength factor α_2 can be represented as $\alpha_2 = 1 + \delta \cdot D$, where $\delta = 0.02/D_{\max}$.

In summary, the final watermark strength factor α can be calculated as:

$$\alpha = (\alpha - c \times \exp(-\xi \cdot E_{HF})) \times \left(1 + \frac{0.02}{D_{\max}} \cdot D\right) - \alpha_0, \quad (8)$$

where α_0 denotes a positive constant, and α_0 is subtracted in this work to control the degree of image distortion after the watermark embedding. In this manner, the value of α_0 can be set to 1.0 in this work.

On the basis of the above analysis, texture masking and visual saliency can be utilized to calculate the strength factor. This strength factor can adaptively change with the change of image texture and the degree of saliency. In this manner, the strength of the embedding can be controlled more appropriately, thus further improving watermarking performance.

3.3. Watermark Detection

The effect of attacks at the receiver can simply be modeled as an additive white Gaussian noise (AWGN) [16]. Furthermore, the complex wavelet coefficients of the low frequency sub-band can be modeled by a Gaussian distribution. The distribution of watermark information “1” or “0” can be represented as follows:

$$y_{i|1} = (1 + \alpha) \cdot x_i + n_i \Rightarrow y_{i|1} \in N((1 + \alpha)\mu, \sigma_{y|1}^2), \quad (9)$$

$$y_{i|0} = (1 - \alpha) \cdot x_i + n_i \Rightarrow y_{i|0} \in N((1 - \alpha)\mu, \sigma_{y|0}^2), \quad (10)$$

where $\sigma_{y|1}^2 = (1 + \alpha)^2 \sigma^2 + \sigma_n^2$, $\sigma_{y|0}^2 = (1 - \alpha)^2 \sigma^2 + \sigma_n^2$, σ_n^2 is the variance of the noise in the related sub-band coefficients.

Complex wavelet coefficients are assumed to be independent and identically distributed in this work. Therefore, the distribution of these coefficients in a specific block with N coefficients y_1, y_2, \dots, y_N for embedding “1” is:

$$f(y_1, y_2, \dots, y_N|1) = \prod_{i=1}^N \frac{1}{\sqrt{2\pi}\sigma_{y|1}} \exp\left(-\frac{(y_i - (1 + \alpha)\mu)^2}{2 \cdot \sigma_{y|1}^2}\right). \quad (11)$$

Similarly, to embed “0”, we have:

$$f(y_1, y_2, \dots, y_N|0) = \prod_{i=1}^N \frac{1}{\sqrt{2\pi}\sigma_{y|0}} \exp\left(-\frac{(y_i - (1 - \alpha)\mu)^2}{2 \cdot \sigma_{y|0}^2}\right). \quad (12)$$

According to the ML decision criterion, the watermark extraction process can be written as follows:

$$f(y_1, y_2, \dots, y_N|1) > f(y_1, y_2, \dots, y_N|0), \quad \hat{w} = 1, \quad (13)$$

$$f(y_1, y_2, \dots, y_N|1) < f(y_1, y_2, \dots, y_N|0), \quad \hat{w} = 0. \quad (14)$$

Thus, by substituting (11) and (12) in (13) and (14), we have:

$$\prod_{i=1}^N \frac{1}{\sqrt{2\pi}\sigma_{y|1}} \exp\left(-\frac{(y_i - (1 + \alpha)\mu)^2}{2 \cdot \sigma_{y|1}^2}\right) > \prod_{i=1}^N \frac{1}{\sqrt{2\pi}\sigma_{y|0}} \exp\left(-\frac{(y_i - (1 - \alpha)\mu)^2}{2 \cdot \sigma_{y|0}^2}\right), \quad \hat{w} = 1, \quad (15)$$

$$\prod_{i=1}^N \frac{1}{\sqrt{2\pi}\sigma_{y|1}} \exp\left(-\frac{(y_i - (1 + \alpha)\mu)^2}{2 \cdot \sigma_{y|1}^2}\right) < \prod_{i=1}^N \frac{1}{\sqrt{2\pi}\sigma_{y|0}} \exp\left(-\frac{(y_i - (1 - \alpha)\mu)^2}{2 \cdot \sigma_{y|0}^2}\right), \quad \hat{w} = 0. \quad (16)$$

We take the logarithm of both sides by calculating:

$$\omega_1 \sum_{i=1}^N y_i^2 + \omega_2 \sum_{i=1}^N y_i > \tau, \quad \hat{w} = 1, \quad (17)$$

$$\omega_1 \sum_{i=1}^N y_i^2 + \omega_2 \sum_{i=1}^N y_i < \tau, \quad \hat{w} = 0, \quad (18)$$

where $\omega_1 = \left(\frac{1}{\sigma_{y|0}^2} - \frac{1}{\sigma_{y|1}^2}\right)$, $\omega_2 = -2(1 + \alpha) \left(\frac{1 - \alpha}{\sigma_{y|0}^2} - \frac{1 + \alpha}{\sigma_{y|1}^2}\right)$.

Therefore, the watermark detection threshold can be expressed as:

$$\tau = 2N \ln\left(\frac{\sigma_{y|1}}{\sigma_{y|0}}\right) - N(1 + \alpha)^2 \left(\frac{(1 - \alpha)^2}{\sigma_{y|0}} - \frac{(1 + \alpha)^2}{\sigma_{y|1}}\right). \quad (19)$$

4. Experimental Results

4.1. Imperceptibility of Watermarking

To assess the performance of the proposed watermarking method, experiments are conducted by using real images. In this study, we used eight natural images (Barbara, Boat, Bridge, Elaine, Lena, Man, Mandrill, and Peppers), each with a size of 512×512 . The host images and their watermarked version with 16×16 blocks and 128-bit message are shown in Figure 4. Throughout the experiments, three level DT-CWT was used to decompose each selected block, and the filters used were the near-symmetric 13, 19 tap filters and Q-shift 14, 14 tap filters. The watermark strength factor α was set to 0.0153 according to Equation (8) in Section 3.2. For each image in Figure 4, the top image is the host image, the middle image the watermarked image, and the bottom image the difference image between the host image and the watermarked version.



Figure 4. Host, watermarked, and difference images: Barbara, Boat, Bridge, Elaine, Lena, Man, Mandrill, and Peppers.

From Figure 4, the watermark imperceptibility is satisfied. The proposed watermarking method provided an image dependent watermark with strong components in the complex part of the image, which is barely noticeable to the human eyes. This scheme allowed for the setting of the high watermark strength factor, while the visual quality of the watermarked image was kept at an acceptable level. Moreover, the peak signal-to-noise-ratio (PSNR) and the structural similarity index measure (SSIM) [43] were used to evaluate the performance of the proposed watermarking method in a subjective manner. The results are shown Table 1, in which the watermarking evaluation results are satisfactory. Therefore, the embedded watermarks were perceptually invisible.

Table 1. Evaluation results with different watermark lengths.

Image	Watermark Length 128		Watermark Length 1024	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM
Barbara	51.1151	0.9999	42.4725	0.9959
Boat	51.6759	0.9998	41.8977	0.9952
Bridge	51.4628	0.9999	42.7279	0.9979
Elaine	51.1990	0.9995	41.4759	0.9938
Lena	52.2745	0.9998	46.0169	0.9931
Man	53.0835	0.9999	48.8653	0.9995
Mandrill	53.0835	0.9999	48.8653	0.9995
Peppers	51.5919	0.9996	42.2739	0.9939

4.2. Error of Probability Analysis

The error probability in the presence of AWGN was derived as follows. Error occurred whenever watermark information “1” was embedded into the host image, while watermark information “0” was extracted at the decoder end, and vice versa. The error probability of the watermarking included these two errors.

According to Equation (17), the error probability of embedding watermark information “1” was:

$$f_{e|1} = f \left(\omega_1 \sum_{i=1}^N y_i^2 + \omega_2 \sum_{i=1}^N y_i < \tau | 1 \right), \quad (20)$$

where $\tau = 2N \ln \left(\frac{\sigma_{y|1}}{\sigma_{y|0}} \right) - N(1+\alpha)^2 \left(\frac{(1-\alpha)^2}{\sigma_{y|0}^2} - \frac{(1+\alpha)^2}{\sigma_{y|1}^2} \right)$, $\omega_1 = \left(\frac{1}{\sigma_{y|0}^2} - \frac{1}{\sigma_{y|1}^2} \right)$, and $\omega_2 = -2(1+\alpha) \left(\frac{1-\alpha}{\sigma_{y|0}^2} - \frac{1+\alpha}{\sigma_{y|1}^2} \right)$. According to previous results [16], $f_{e|1}$ can be written as:

$$f_{e|1} = \frac{1}{\sqrt{2\pi N \sigma_{y|1}^2}} \cdot \frac{\kappa_1}{\kappa_2} \times \int_0^\infty \gamma \left(\frac{N}{2}, \frac{x}{2} \right) \cdot \exp \left(\frac{-(\tilde{\tau} - \kappa_1 x / \kappa_2 - N(1+\alpha)\mu)}{2N\sigma_{y|1}^2} \right) dx, \quad (21)$$

where $\kappa_1 = \omega_1 \sigma_{y|1}^2$, $\kappa_2 = 2(1+\alpha)\mu\omega_1 + \omega_2$, $\tilde{\tau} = \tau + \omega_1 N(1+\alpha)^2 \mu^2$, and $\gamma \left(\frac{N}{2}, \frac{x}{2} \right)$ denotes a Gamma function.

Meanwhile, the error probability of embedding watermark information “0” is:

$$f_{e|0} = f \left(\omega_1 \sum_{i=1}^N y_i^2 + \omega_2 \sum_{i=1}^N y_i > \tau | 0 \right). \quad (22)$$

According to [16], $f_{e|0}$ can be further written as:

$$f_{e|0} = 1 - \frac{c_1}{c_2 \sqrt{2\pi N \sigma_{y|0}^2}} \cdot \int_0^\infty \gamma \left(\frac{N}{2}, \frac{x}{2} \right) \cdot \zeta(x) dx, \quad (23)$$

where $c_1 = \omega_1 \sigma_{y|0}^2$, $\sigma_{y|0}^2 = (1 - \alpha)^2 \sigma^2 + \sigma_n^2$, $c_2 = 2(1 - \alpha) \mu \omega_1 + \omega_2$, $\hat{\tau} = \tau + \omega_1 N(1 - \alpha)^2 \mu^2$, $\zeta(x) = \exp\left(\frac{-(\hat{\tau} - c_1 x / c_2 - N(1 - \alpha) \mu)}{2N\sigma_{y|0}^2}\right)$.

The data bits “0” and “1” were assumed to be inserted in the original image with equal probabilities. On the basis of Equations (21) and (23), the total error probability can be written as:

$$F_e = 0.5f_{e|1} + 0.5f_{e|0} \quad (24)$$

Figure 5 shows the error probability F_e versus the different values of noise variance for the Lena image under AWGN attack. From Figure 5, although the error probability F_e increased with the increase of noise variance, the change value of error probability remained small as the noise attack strength increased.

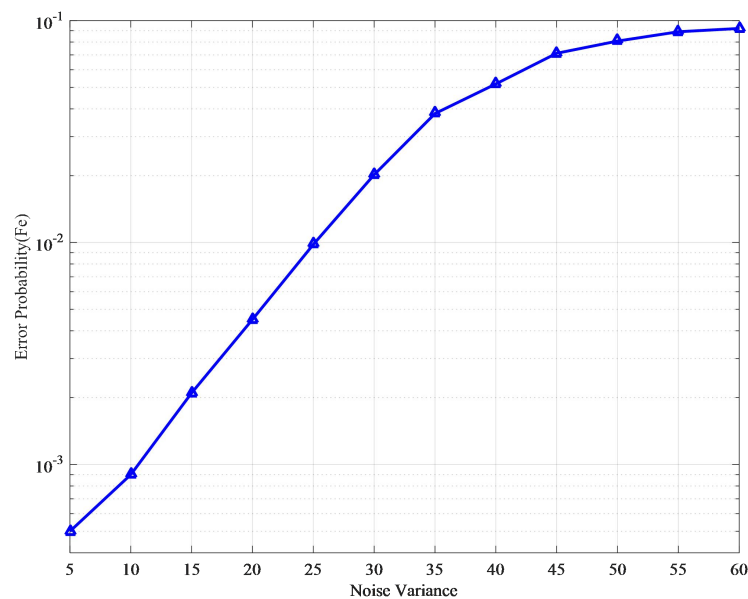


Figure 5. Error probability (F_e) versus noise variance for AWGN attack.

4.3. Performance under Attacks

For testing robustness, several common attacks, as described by [16,28], were utilized for the watermarked images by the proposed method. These attacks included common image processing attacks and geometric distortion attacks. In this study, bit-error rate (BER) was used to evaluate the robustness of the watermarking under several intentional or unintentional attacks. To save on space, the robustness of the proposed method under AWGN, median filtering, Gaussian filtering, JPEG compression, scaling attack, rotation attack, and combinational attack on the eight well known images (i.e., Barbara, Boat, Bridge, Elaine, Lena, Man, Mandrill, and Peppers) was investigated.

(1) AWGN attack:

Figure 6 shows the results of BER of various test images against AWGN attacks. When the noise variance was less than 10, BER was near zero. When noise variance was less than 33, the corresponding BER was near 0.1. Therefore, the proposed watermarking had good robustness against AWGN attacks.

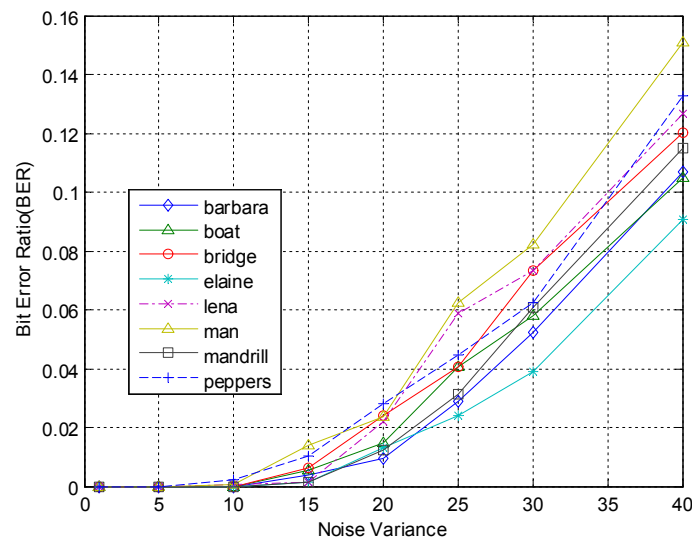


Figure 6. AWGN attack with different noise variances.

(2) JPEG compression attack:

Figure 7 shows the results of BER against JPEG compression attacks, in which the proposed watermarking demonstrates robustness, even if the quality factor is very low (e.g., quality factor of five). When the strength of the JPEG compression attack was very large (e.g., quality factor of five), the result of BER was less than 0.3. When the JPEG compression quality factor was greater than 25, BER tended to be zero. Therefore, the proposed watermarking algorithm was robust against JPEG compression attacks.

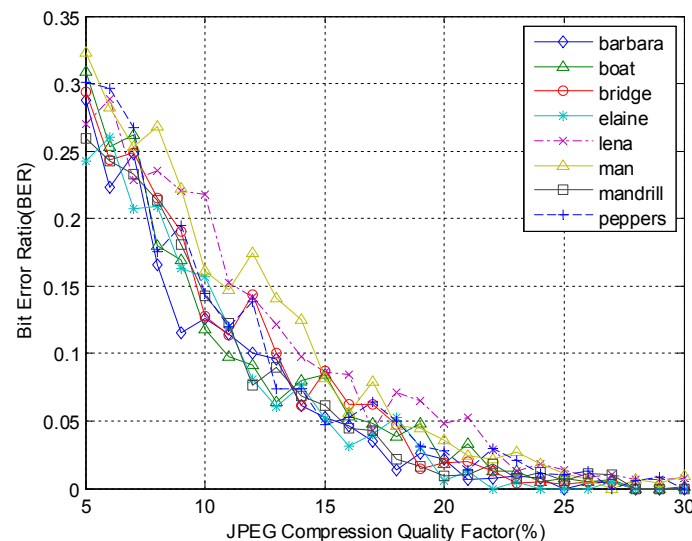


Figure 7. JPEG attack for various test images with different quality factors.

(3) Scaling attack:

Table 2 shows the BER results under amplitude scaling attacks. The watermarking algorithm was robust to most scaling attacks. However, Table 2 also shows that when the scaling factor was equal to 0.7 or 1.1, BER had a comparatively large value. The reason is not yet clear, and this issue will be explored in our future work.

Table 2. BER results of the extracted watermark under scaling attack.

Image	Scaling Factor										
	0.5	0.7	0.75	0.8	0.9	1.1	1.2	1.3	1.4	1.5	2.0
Barbara	0.0086	0.1868	0	0.0789	0.0164	0.1422	0.0820	0.0531	0	0	0
Boat	0	0.3141	0	0.1984	0.0336	0.2781	0.1883	0.0945	0	0	0
Bridge	0	0.1547	0	0.0719	0.0086	0.1250	0.0828	0.0336	0	0	0
Elaine	0	0.2750	0	0.1430	0.0383	0.2297	0.1406	0.0672	0.0047	0	0
Lena	0	0.2210	0	0.1289	0.0195	0.1828	0.1250	0.0680	0.0047	0	0
Man	0	0.2617	0	0.1273	0.0234	0.2336	0.1289	0.0586	0.0063	0	0
Mandrill	0.0016	0.1172	0	0.0195	0	0.0836	0.0234	0.0047	0	0	0
Peppers	0	0.2688	0	0.1563	0.0258	0.2398	0.1555	0.0570	0.0078	0	0

(4) Rotation attack:

Table 3 shows the results of the BER of various test images against rotation attacks. The range of the rotation angle was $[-10^\circ, 10^\circ]$. When the range of the rotation angle was $[-5^\circ, 5^\circ]$, the range of the BER was $[0, 0.07]$. Among the values listed in in Table 3, the maximum BER was 0.1016, whereas most of the other BER values were small. The effect of BER was not prominent when the angle increased. Thus, the proposed embedding approach was robust against rotation attacks.

Table 3. BER results of the extracted watermark under rotation attack.

Image	Rotation Angle									
	-10°	-5°	-2°	-1°	-0.5°	0.5°	1°	2°	5°	10°
Barbara	0.0825	0.0422	0.0422	0.0383	0.0336	0.0186	0.0188	0.0188	0.0297	0.0398
Boat	0.0320	0.0328	0.0289	0.0266	0.0242	0	0	0.0031	0.0078	0.0078
Bridge	0.0430	0.0328	0.0266	0.0266	0.0266	0.0258	0.0320	0.0344	0.0430	0.0594
Elaine	0.0727	0.0344	0.0164	0.0164	0.0164	0.0172	0.0172	0.0172	0.0352	0.0531
Lena	0.0422	0.0188	0.0133	0.0133	0.0133	0.0078	0.0078	0.0078	0.0133	0.0273
Man	0.0320	0.0227	0.0109	0.0109	0.0109	0.0031	0.0031	0.0070	0.0227	0.0328
Mandrill	0.1016	0.0789	0.0617	0.0617	0.0617	0.0359	0.0391	0.0391	0.0476	0.0820
Peppers	0.0398	0.0289	0.0242	0.0195	0.0164	0.0312	0.0359	0.0359	0.0523	0.0516

(5) Gaussian filtering and median filtering attacks:

Table 4 shows the BER results against Gaussian filtering and median filtering attacks. The window sizes of Gaussian filtering and median filtering were 3×3 , 5×5 , and 7×7 . The proposed method was highly robust against Gaussian filtering attacks. When the window size of the median filtering was 3×3 , the performance of the proposed scheme was robust. However, with the increase of the window size of the median filtering, the robustness of the watermarking was decreased.

Table 4. BER results of the extracted watermark under Gaussian filtering and median filtering attacks.

Image	Gaussian Filtering			Median Filtering		
	3×3	5×5	7×7	3×3	5×5	7×7
Barbara	0.0375	0.0535	0.0535	0.0562	0.1734	0.2757
Boat	0.0176	0.0320	0.0340	0.0671	0.1902	0.2820
Bridge	0.0512	0.0664	0.0672	0.1316	0.2668	0.3422
Elaine	0.0227	0.0316	0.0332	0.0020	0.0309	0.1129
Lena	0.0301	0.0410	0.0430	0.0652	0.1836	0.2566
Man	0.0531	0.0754	0.0785	0.0715	0.2020	0.2793
Mandrill	0.0535	0.0750	0.0750	0.2035	0.3074	0.3555
Peppers	0.0297	0.0449	0.0469	0.0227	0.0668	0.1707

(6) Combinational attack:

Table 5 shows the BER results under the combinational attack for various distortions associated with JPEG compression with a quality factor of 20%. The robustness of the proposed method against this kind of combinational attack was satisfactory. The result of BER against Gaussian noise attack combined with JPEG compression attack for different images is shown in Figure 8, which further confirmed that the proposed scheme had good robustness for this kind of combinational attack.

Table 5. BER results under JPEG compression (quality factor = 20%) combined with other attacks.

Method	Barbara	Boat	Peppers	Elaine	Bridge	Mandrill
JPEG and Scaling (0.75)	0	0.0078	0	0.0078	0	0.0078
JPEG and Scaling (0.90)	0.0187	0.0078	0	0.0178	0.0078	0.0239
JPEG and Scaling (1.10)	0.0781	0.0356	0.0313	0.0664	0.1253	0.0907
JPEG and Gaussian filtering (3×3)	0.0586	0.0313	0.0295	0.0352	0.0519	0.0643
JPEG and Gaussian filtering (5×5)	0.0586	0.0508	0.0364	0.0469	0.0741	0.0852
JPEG and Median filtering (3×3)	0.0591	0.0710	0.0390	0.1168	0.0078	0.2015
JPEG and Median filtering (5×5)	0.1476	0.1592	0.1187	0.2375	0.0352	0.2848

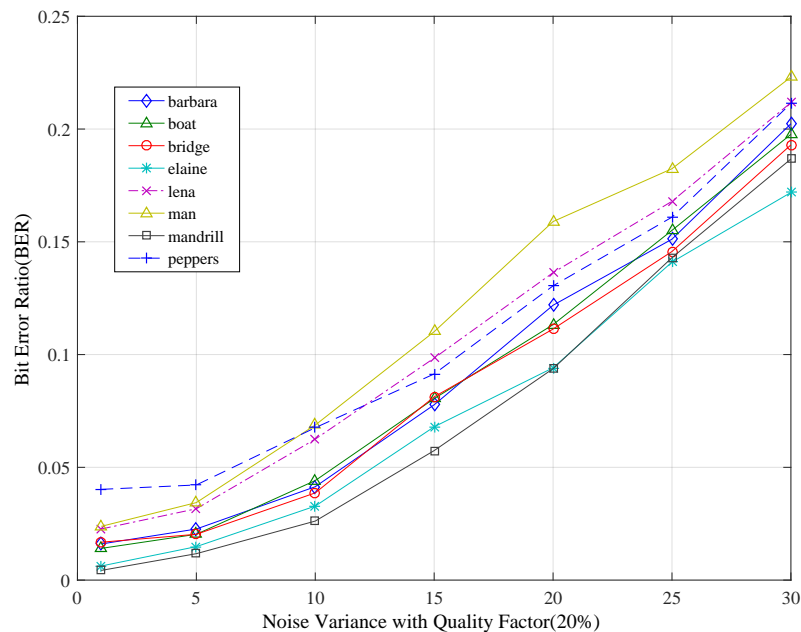


Figure 8. Results for JPEG compression (quality factor = 20%) attack combined with AWGN attack for various test images with different noise variances.

4.4. Comparison with Other Methods

In this part of the study, our method is compared with its most related competitors, particularly the methods reported in [16,28,44,45]. The methods in [16,44] were chosen on the basis of their similarity with the proposed watermarking. For example, the methods all used high entropy image blocks of an original image for watermark embedding. To ensure fairness in comparison, the message lengths and PSNR values used in our experiments were the same as those in the other works. The results in Table 6 depict the same watermark lengths of 256 bits embedded into Barbara, Boat, and Peppers images, while the PSNR of the watermarked image was 45 dB. The results of our method were better than those in the other works for most attacks. For instance, for geometric attacks, such as scaling and rotation attacks, the proposed method outperformed the above three watermarking methods. The main reason was that DT-CWT can effectively approximate shift invariances for geometric transformations. However, the proposed method was slightly ineffective compared to the methods in [28,44] under

AWGN attacks. This problem will be investigated thoroughly by studying the statistical properties of DT-CWT coefficients and noise in our future work.

Table 6. BER (%) results of the extracted watermark under some common attack.

Method	AWGN $\sigma_n = 20$	Median 3×3	Gaussian 3×3	JPEG 10%	Scaling 0.9	Rotation -5°	Rotation 5°
Test image Barbara							
Akhaee [16]	6.33	7.06	3.16	7.80	2.79	3.92	2.36
Kalantari [28]	0.19	20.47	5.29	7.03	6.11	9.04	10.09
Yadav [44]	0	0.78	0.39	11.72	0.32	6.27	7.35
Proposed	2.15	2.73	1.17	2.73	0	3.52	2.34
Test image Boat							
Akhaee [16]	9.54	11.11	5.46	16.39	4.46	3.09	0.35
Kalantari [28]	0	14.38	8.31	9.64	8.23	8.98	9.40
Yadav [44]	2.34	1.95	1.17	9.37	0.16	5.74	6.03
Proposed	2.58	2.73	0	2.73	0.78	1.95	0.78
Test image Peppers							
Akhaee [16]	11.23	2.78	3.26	17.25	1.27	3.40	4.80
Kalantari [28]	0	3.44	6.19	8.07	7.22	9.15	11.34
Yadav [44]	1.56	0.78	1.95	10.93	0.24	6.90	8.85
Proposed	2.81	0.78	1.17	4.30	0.39	2.73	3.52

Tables 7 and 8 show the BER results against median filtering attack and JPEG compression attack by using the proposed method and those methods in [28,44], in which the watermark length was 256 bits and the PSNR of the watermarked image was 45 dB, respectively. As shown in both tables, the proposed method had better results than the methods in [28,44].

Table 7. BER (%) comparison of the recovered watermark under median filtering attack.

Image	Kalantari [28]			Proposed Method		
	Median Filtering			Median Filtering		
	3×3	5×5	7×7	3×3	5×5	7×7
Lena	10.16	21.48	28.52	2.73	13.67	18.75
Peppers	3.44	14.45	25.07	0.78	3.91	14.84
Boat	14.38	26.10	37.89	2.73	13.28	22.66

Table 8. BER (%) comparison of the recovered watermark under JPEG compression attack.

Method	Image	JPEG Compression Quality Factor (%)				
		10	20	30	40	50
Kalantari [28]	Lena	9.24	1.74	0.78	0.13	0
Yadav [44]	Lena	18.75	8.98	4.30	0.78	0
Proposed	Lena	6.25	0	0	0	0
Kalantari [28]	Peppers	8.07	2.21	0.78	0.26	0
Yadav [44]	Peppers	10.94	3.91	1.17	0.78	0.39
Proposed	Peppers	4.30	0.39	0.39	0	0
Kalantari [28]	Boat	9.64	1.56	0.39	0	0
Yadav [44]	Boat	9.37	6.25	1.72	0.39	0
Proposed	Boat	2.73	0	0.39	0	0

Table 9 shows the BER results under scaling attack with a watermark length of 100 bits and a PSNR of the watermarked image of 45 dB. The results of the proposed method outperformed those

of the methods in [44,45] for most scaling attack. As described in the third part of Section 4.2 (i.e., “scaling attack”), when the scaling factor was equal to 0.7 or 1.1, the robustness of the watermarking decreased dramatically. We will investigate this issue in our future work.

Table 9. BER (%) comparison of the recovered watermark under scaling attack.

Method		Scaling Factor					
		0.5	0.7	0.9	1.1	1.3	1.5
Yadav [44]	Lena	1.0	20.0	10.0	6.0	0	0
Tsougenis [45]	Lena	5.0	3.0	4.0	8.0	8.0	12.0
Proposed method	Lena	0	11.7	1.90	7.7	7.0	0
Yadav [44]	Peppers	0	13.0	6.0	1.0	0	0
Tsougenis [45]	Peppers	13.0	5.0	8.0	17.0	17.0	20.0
Proposed method	Peppers	0	11.4	3.0	10.0	0	0

5. Conclusions

An image watermarking method was proposed in this study by using DT-CWT and the multiplicative strategy. In this approach, after partitioning a host image into non-overlapping blocks, the high entropy image blocks were selected for watermark embedding. Watermark data extraction was performed by using the MLE decision criterion, and the embedding factor was computed to improve the robustness of the watermarking by using the texture masking and visual saliency scheme. The performance of the proposed scheme was evaluated in terms of image quality and robustness. The experimental results demonstrated the effectiveness of the proposed method.

Author Contributions: J.L. conceived of the idea, designed the experiments, and wrote the manuscript; Y.R. helped to revise this manuscript; Y.H. helped to test and analyze the experimental data.

Funding: This work was supported by the Science and Technology Foundation of Jiangxi Provincial Education Department (Grant No. GJJ170922) and the Natural Science Foundation of Jiangxi (No. 20192BAB207013).

Conflicts of Interest: The authors declare no conflict of interest.

References

- Asikuzzaman, M.; Pickering, M.R. An overview of digital video watermarking. *IEEE Trans. Circuit. Syst. Video Technol.* **2018**, *28*, 2131–2153. [\[CrossRef\]](#)
- Wang, Y.G.; Zhou, G.P.; Shi, Y.Q. Transportation spherical watermarking. *IEEE Trans. Image Process.* **2018**, *27*, 2063–2077. [\[CrossRef\]](#) [\[PubMed\]](#)
- Jang, B.-G.; Lee, S.-H.; Lee, Y.-S.; Kwon, K.-R. Biological viral infection watermarking architecture of MPEG/H.264/AVC/HEVC. *Electronics* **2019**, *8*, 889. [\[CrossRef\]](#)
- Guo, Y.F.; Au, O.C.; Wang, R.; Fang, L.; Cao, X.C. Halftone image watermarking by content aware double-sided embedding error diffusion. *IEEE Trans. Image Process.* **2018**, *27*, 3387–3402. [\[CrossRef\]](#)
- Ou, B.; Li, L.; Zhao, Y.; Ni, R. Efficient color image reversible data hiding based on channel-dependent payload partition and adaptive embedding. *Signal Process.* **2015**, *108*, 642–657. [\[CrossRef\]](#)
- Cox, I.J.; Kilian, J.; Leighton, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.* **1997**, *6*, 1673–1687. [\[CrossRef\]](#)
- Liu, X.; Han, G.; Wu, J.; Shao, Z.; Coatrieux, G.; Shu, H. Fractional krawtchouk transform with an application to image watermarking. *IEEE Trans. Signal Process.* **2017**, *65*, 1894–1908. [\[CrossRef\]](#)
- Ahmaderaghi, B.; Kurugollu, F.; Rincon, J.M.D.; Bouridane, A. Blind image watermark detection algorithm based on discrete shearlet transform using statistical decision theory. *IEEE Trans. Comput. Imaging* **2018**, *4*, 46–59. [\[CrossRef\]](#)
- Singh, D.; Singh, S.K. DCT based efficient fragile watermarking scheme for image authentication and restoration. *Multimed. Tools Appl.* **2017**, *76*, 953–977. [\[CrossRef\]](#)

10. Rahman, M.M.; Ahmad, M.O.; Swamy, M.N.S. A new statistical detector for DWT-based additive image watermarking using the Gaussian–Hermite expansion. *IEEE Trans. Image Process.* **2009**, *18*, 1782–1796. [[CrossRef](#)]
11. Sadreazami, H.; Ahmad, M.O.; Swamy, M.N.S. A study of multiplicative watermark detection in the contourlet domain using alphasstable distributions. *IEEE Trans. Image Process.* **2014**, *23*, 4348–4360. [[CrossRef](#)] [[PubMed](#)]
12. Amini, M.; Ahmad, M.O.; Swamy, M.N.S. A robust multibit multiplicative watermark decoder using a vector based hidden markov model in wavelet domain. *IEEE Trans. Circuit. Syst. Video Technol.* **2018**, *28*, 402–413. [[CrossRef](#)]
13. Hwang, M.J.; Lee, J.S.; Lee, M.S.; Kang, H.G. SVD based adaptive QIM watermarking on stereo audio signals. *IEEE Trans. Multimed.* **2018**, *20*, 45–54. [[CrossRef](#)]
14. Zareian, M.; Tohidypour, H.R. A novel gain invariant quantization-based watermarking approach. *IEEE Trans. Inf. Forensics Sec.* **2014**, *9*, 1804–1813. [[CrossRef](#)]
15. Sadreazami, H.; Amini, A. A robust spread spectrum based image watermarking in ridgelet domain. *Int. J. Electron. Commun.* **2012**, *66*, 364–371. [[CrossRef](#)]
16. Akhaee, M.A.; Sahraeian, S.M.E.; Sankur, B.; Marvasti, F. Robust Scaling-based image watermarking using maximum-likelihood decoder with optimum strength factor. *IEEE Trans. Multimed.* **2009**, *11*, 822–833. [[CrossRef](#)]
17. Liu, J.H.; She, K. A hybrid approach of DWT and DCT for rational dither modulation watermarking. *Circuits Syst. Signal Process.* **2012**, *31*, 797–811. [[CrossRef](#)]
18. You, X.; Du, L.; Cheung, Y.M.; Chen, Q.H. A blind watermarking scheme using new nontensor product wavelet filter banks. *IEEE Trans. Image Process.* **2010**, *19*, 3271–3284. [[CrossRef](#)]
19. Ramanjaneyulu, K.; Rajarajeswari, K. Wavelet based oblivious image watermarking scheme using genetic algorithm. *IET Image Process.* **2012**, *6*, 364–373. [[CrossRef](#)]
20. Barni, M.; Bartolini, F.; Piva, A. Improved wavelet-based watermarking through pixel-wise masking. *IEEE Trans. Image Process.* **2001**, *10*, 783–791. [[CrossRef](#)]
21. Bhowmik, D.; Abhayaratne, C. Quality scalability aware watermarking for visual content. *IEEE Trans. Image Process.* **2016**, *25*, 5158–5172. [[CrossRef](#)] [[PubMed](#)]
22. Wang, J.; Lian, S.; Shi, Y.Q. Hybrid multiplicative multiwatermarking in DWT domain. *Multidimens. Syst. Signal Process.* **2017**, *28*, 617–636. [[CrossRef](#)]
23. Xiong, L.; Xu, Z.; Shi, Y.Q. An integer wavelet transform based scheme for reversible data hiding in encrypted images. *Multidimens. Syst. Signal Process.* **2018**, *29*, 1191–1202. [[CrossRef](#)]
24. Yu, X.Y.; Wang, C.Y.; Zhou, X. A hybrid transforms based robust video zero-watermarking algorithm for resisting high efficiency video coding compression. *IEEE Access* **2019**, *7*, 115708–115724. [[CrossRef](#)]
25. Langelaar, G.C.; Setyawan, I.; Lagendijk, R.L. Watermarking digital image and video data: A state-of-the-art overview. *IEEE Trans. Signal Process. Mag.* **2000**, *17*, 20–26. [[CrossRef](#)]
26. Cheng, Q.; Huang, T.S. Robust optimum detection of transform domain multiplicative watermarks. *IEEE Trans. Signal Process.* **2003**, *51*, 906–924. [[CrossRef](#)]
27. Do, M.N.; Vetterli, M. The contourlet transform: an efficient directional multi-resolution image processing. *IEEE Trans. Image Process.* **2005**, *14*, 2091–2106. [[CrossRef](#)]
28. Kalantari, N.K.; Ahadi, S.M.; Vafadust, M. A robust image watermarking in the ridgelet domain using universally optimum decoder. *IEEE Trans. Circuit. Syst. Video Technol.* **2010**, *20*, 396–406. [[CrossRef](#)]
29. Demanet, L.; Ying, L.X. Wave atoms and time upscaling of wave equations. *Numer. Math.* **2009**, *13*, 1–71. [[CrossRef](#)]
30. Sadreazami, H.; Ahmad, O.; Swamy, M.N.S. Multiplicative watermark decoder in contourlet domain using the normal inverse Gaussian distribution. *IEEE Trans. Multimed.* **2016**, *18*, 196–207. [[CrossRef](#)]
31. Wang, F.; Zhao, X.L.; Ng, M. Multiplicative noise and blur removal by framelet decomposition and L_1 based L -curve method. *IEEE Trans. Image Process.* **2016**, *25*, 4222–4232. [[CrossRef](#)]
32. Selesnick, I.W.; Baraniuk, R.G.; Kingbury, N.G. The dual-tree complex wavelets transform—A coherent framework for multi-scale signal and image processing. *IEEE Signal Process. Mag.* **2005**, *22*, 123–151. [[CrossRef](#)]
33. Liu, J.H.; Xu, Y.Y.; Wang, S.; Zhu, C. Complex wavelet domain image watermarking algorithm using L_1 norm function-based quantization. *Circuits Syst. Signal Process.* **2018**, *37*, 1268–1286. [[CrossRef](#)]

34. Celik, T.; Ma, K.K. Unsupervised change detection for satellite images using dual-tree complex wavelet transform. *IEEE Trans. Geosci. Remote Sens.* **2010**, *48*, 1199–1210. [[CrossRef](#)]
35. Watson, A.B.; Yang, G.Y.; Solomon, J.A.; Villasenor, J. Visibility of wavelet quantization noise. *IEEE Trans. Image Process.* **1997**, *6*, 1164–1175. [[CrossRef](#)]
36. Yang, X.; Lin, W.; Liu, Z.; Ongg, Z.; Yao, S. Motion-compensated residue preprocessing in video coding based on just-noticeable-distortion profile. *IEEE Trans. Circuits Syst. Video Technol.* **2005**, *15*, 745–752.
37. Wang, C.; Zhang, T.; Wan, W.; Han, X.; Xu, M. A novel STDM watermarking using visual saliency based JND model. *Information* **2017**, *8*, 103. [[CrossRef](#)]
38. Wang, C.; Han, X.; Wan, W.; Li, J.; Sun, J.; Xu, M. Visual saliency based just noticeable difference estimation in DWT domain. *Information* **2018**, *9*, 178. [[CrossRef](#)]
39. Akhaee, M.A.; Sahraeian, S.M.; Marvasti, F. Contourlet based image watermarking using optimum detector in a noisy environment. *IEEE Trans. Image Process.* **2010**, *19*, 967–980. [[CrossRef](#)]
40. Papakostas, G.A.; Tsougenis, E.D.; Koulouriotis, D.E. Fuzzy knowledge based adaptive image watermarking by the method of moments. *Complex Intell. Syst.* **2016**, *2*, 205–220. [[CrossRef](#)]
41. Borji, A.; Itti, L. State-of-the-art in visual attention modeling. *IEEE Trans. Pattern Anal. Mach. Intell.* **2013**, *35*, 185–207. [[CrossRef](#)] [[PubMed](#)]
42. Borji, A.; Sihite, D.N.; Itti, L. Quantitative analysis of human model agreement in visual saliency modeling: A comparative study. *IEEE Trans. Image Process.* **2013**, *22*, 55–69. [[CrossRef](#)] [[PubMed](#)]
43. Wang, Z.; Bovik, A.C.; Sheikh, H.R. Image quality assessment from error visibility to structural similarity. *IEEE Trans. Image Process.* **2004**, *13*, 600–612. [[CrossRef](#)] [[PubMed](#)]
44. Yadav, N.; Singh, K. Robust image-adaptive watermarking using an adjustable dynamic strength factor. *Signal Image Video Process.* **2015**, *9*, 1531–1542. [[CrossRef](#)]
45. Tsougenis, E.D.; Papakostas, G.A.; Koulouriotis, D.E.; Tourassis, V.D. Towards adaptivity of image watermarking in polar harmonic transforms domain. *Opt. Laser Technol.* **2013**, *54*, 84–97. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).